UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/792,325	03/02/2004	Mauricio Sanchez	200316381-1	4396

22879 7590 05/15/2008
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
JEAN GILLES, JUDE	

ART UNIT	PAPER NUMBER
2143	

NOTIFICATION DATE	DELIVERY MODE
05/15/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	**Application No.** 10/792,325	**Applicant(s)** SANCHEZ, MAURICIO	
	Examiner JUDE J. JEAN GILLES	**Art Unit** 2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _02 March 2004_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-49_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-49_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _02 March 2004_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _03/02/2004_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This Office Action is responsive to communication filed on 03/02/2004.

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on 03/02/2004 has been considered by the examiner.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

3. Claims 1-8, 12-14, 20-29, 32-42, 44-46, and 48-49 rejected under 35 U.S.C. 102(e) as being anticipated by Dent et al (Dent), U.S. Pub. No. 2003/0036359 A1.

Regarding claims 1-8, 12-14, 20-29, 32-42, 44-46, and 48-49, Dent discloses:

1. A computing device (*see abstract; processing system 18*), comprising:

a processor (*fig. 2, item 30, 32*); a memory coupled to the processor (*fig. 2, item 34*); and program instructions provided to the memory and executable by the processor (*par. 0049*) to:

transmit a network management message over a network to a network device (*par. 0051; see transmitting the message to the receivers*);

collect response information from the network device based on the network management message (*par. 0068; 0180*); and

analyze the response information including applying a Kalman filter to the collected response information (*par. 0014; 0151; 0176-0177, and 0188*).

2. The device of claim 1, wherein the computing device is a network event regulator device (0052, 0069, 0153).

3. The device of claim 2, wherein the computing device is selected from the group of a wireless access point, a switch, a hub, and a router (0048).

4. The device of claim 1, further including program instructions which execute to regulate external network stimuli based on applying the Kalman filter to reduce degraded performance to the network (*par. 0014; 0151; 0176-0177, and 0188*).

5. The device of claim 1, further including program instructions which execute to signal when abnormal levels of activity are detected based on applying the Kalman filter (*par. 0014; 0151; 0176-0177, and 0188*).

6. The device of claim 1, further including program instructions which execute to track

media access control (MAC) layer addressing and which execute to learn network events based on applying the Kalman filter as other devices connect to the network (*par. 0048; 0014; 0151; 0176-0177, and 0188; inherently, the use of the Kalman filter and specifically having the Kalman Tracker enables tracking of MAC layer addressing*).

7. The device of claim 1, further including program instructions which execute to track internet protocol (IP) flow and routing and which execute to learn network events based on applying the Kalman filter as other devices connect to the network (par. 0047-0048; *par. 0014; 0151; 0176-0177, and 0188*).

8. The device of claim 7, further including program instructions which execute to track IP flow and routing at a network device selected from the group of a switch, a hub, a database, a security appliance, a wireless access point device, a network intrusion device, and a router (par. 0047-0048).

12. A computing device(*see abstract; processing system 18*), comprising:

a processor (*fig. 2, item 30, 32*);

a memory coupled to the processor (*fig. 2, item 34*); and

program instructions provided to the memory and executable by the processor (*par. 0049*) to:

collect information from a network device connected to the computing device over a network (*par. 0068; 0180*);

analyze collected information including applying a Kalman filter to the collected response information(*par. 0014; 0151; 0176-0177, and 0188*); and

regulate external network stimuli based on applying the Kalman filter to reduce degraded performance on the network (*par. 0014; 0151; 0176-0177, and 0188*).

13. The computing device of claim 12, further including collecting information from the network device selected from the group of: processor utilization; memory utilization; link up/down status; traps; buffer utilization; local area network (LAN) utilization; and statistics including discards, cyclical redundancy checking (CRC) and frame check sequence (FCS) errors and number of broadcasts (par. 0220).

14. The computing device of claim 12, further including program instructions which execute to automatically calibrate a threshold in the network device used to control a connection rate to the network device (see abstract; par. 0017-0019).

20. The computing device of claim 12, wherein the network device includes a network device selected from the group of: a switch; a hub; a database; a security appliance; a wireless access point device; a network intrusion device; and a router(0048).

21. The computing device of claim 12, wherein the network device and the computing device are connected over a local area network (LAN) (fig. 2 can be configured as LAN).

22. The computing device of claim 12, wherein the network device and the computing device are connected over a wireless wide area network (WAN) (fig. 1)

23. A method for network and network device management, comprising:

receiving network information associated with a network device (*par. 0051; see receiving the message at the receivers*); and

analyzing the network information using a Kalman filter (*par. 0014; 0151; 0176-0177, and 0188*).

24. The method of claim 23, wherein the method includes receiving response information to an SNMP message sent to the network device (0048-0052).

25. The method of claim 23, wherein the method includes receiving information contained in a management information base (MIB) of the network device (0048-0052).

26. The method of claim 23, wherein the method includes using a software agent embedded in the network device to receive and analyze the network information (*par. 0014; 0151; 0176-0177, and 0188*).

27. The method of claim 23, wherein the method includes receiving network information associated with a device selected from the group of a switch, a hub, a database, a security appliance, a wireless access point device, a network intrusion device, and a router (0048).

28. The method of claim 23, wherein the method includes receiving media access control (MAC) layer addressing information (*par. 0048; 0014; 0151; 0176-0177, and 0188; inherently, the use of the Kalman filter and specifically having the Kalman Tracker enables tracking of MAC layer addressing*).

29. The method of claim 23, wherein the method includes receiving internet protocol (IP) flow and routing information (par. 0047-0048; *par. 0014; 0151; 0176-0177, and 0188*).

32. The method of claim 23, wherein the method includes regulating external network stimuli based on applying the Kalman filter to received network information.

33. The method of claim 23, wherein the method includes producing an alert signal when abnormal levels of activity are detected based on analyzing the network information using the Kalman filter.

34. A method for network and network device management (*see abstract; processing system 18*), comprising:

collecting information associated with a network device (*par. 0068; 0180*);

analyzing the collected information including applying a Kalman filter to the collected information (*par. 0014; 0151; 0176-0177, and 0188*); and

regulating external network stimuli based on applying the Kalman filter in order to reduce network performance degradation (*par. 0014; 0151; 0176-0177, and 0188*).

35. The method of claim 34, wherein the method includes receiving media access control (MAC) layer addressing information and learning network events based on applying the Kalman filter to the MAC layer addressing information (*par. 0048; 0014; 0151; 0176-0177, and 0188; inherently, the use of the Kalman filter and specifically having the Kalman Tracker enables tracking of MAC layer addressing*).

36. The method of claim 34, wherein the method includes receiving internet

protocol (IP) flow and route information and learning network events based on applying the Kalman filter to the IP flow and route information (par. 0047-0048; *par. 0014; 0151; 0176-0177, and 0188*).

37. The method of claim 34, wherein the method includes converting the network device from a first role to a second role based on applying the Kalman filter to the collected information (see Tzamaloukas; par. 0033, 0113).

38. The method of claim 34, wherein the method includes automatically calibrating a threshold in the network device used to control a connection rate to the network device based on applying the Kalman filter to the collected information while the network device is in network use (*par. 0014; 0151; 0176-0177, and 0188*).

39. A computer readable medium having instructions for causing a device to perform a method (*see abstract; processing system 18*), comprising:

receiving network information associated with a network device (*par. 0051; see receiving the message at the receivers*); and

analyzing the network information using a Kalman filter (*par. 0014; 0151; 0176-0177, and 0188*).

40. The medium of claim 39, wherein the method further includes automatically

calibrating a threshold in the network device used to control a connection rate to the network device based on applying the Kalman filter to the network information while the network device is in network use (*par. 0014; 0151; 0176-0177, and 0188*).

41. The medium of claim 39, wherein the method further includes learning media access control (MAC) layer addressing events based on applying the Kalman filter to MAC layer addressing information (*par. 0048; 0014; 0151; 0176-0177, and 0188; inherently, the use of the Kalman filter and specifically having the Kalman Tracker enables tracking of MAC layer addressing*).

42. The medium of claim 39, wherein the method further includes learning internet protocol (IP) flow and routing events based on applying the Kalman filter to IP flow and route information (par. 0047-0048; *par. 0014; 0151; 0176-0177, and 0188*).

44. A network device (*see abstract; processing system 18*), comprising: a processor (*fig. 2, item 30, 32*);

a memory coupled to the processor (*fig. 2, item 34*);

means for regulating external network stimuli based on applying a Kalman filter to information associated with the network device (*par. 0014; 0151; 0176-*

0177, and 0188).

45. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes executing a set of program instructions on the network device (*par. 0014; 0151; 0176-0177, and 0188*).

46. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes executing a set of program instructions on another network device connected to the network device over a local area network (*par. 0014; 0151; 0176-0177, and 0188*).

48. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to reduce network performance degradation on the network device (*par. 0014; 0151; 0176-0177, and 0188*).

49. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to reduce network performance degradation on a different network device (*par. 0014; 0151; 0176-0177, and 0188*).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 9-11, 15-19, 30-31, 43, 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dent in view of Tzamaloukas et al (Tzamaloukas) , U.S. pub. 20040073361 A1

Regarding claim 9, Dent teaches the details of the computing device of claim 1 as demonstrated above, but fail to spell out the device of claim 1, further including program instruction which execute to track information between various network layers in a given protocol stack model and which execute to learn network events based on applying the Kalman filter to the tracked information. Nonetheless, this feature is well known and would have been an obvious modification to the system of Dent as evidenced by Tzamaloukas.

In an analogous art, Tzamaloukas teaches a network communication system that provides internal network protocol stack for the mobile communication device (see Tzamaloukas, par. 0056, and 0076-0077; fig. 4). In an attempt to facilitate the tracking of events as thy pertain to particular network devices, this mechanism fits well in the system of Dent. Accordingly, it would have been obvious for an ordinary skill in the art, at the time the invention was made to have incorporated the feature of Tzamaloukas within the structure of Dent for the purpose of exchanging network events such as traffic congestion as stated by Tzamaloukas in par. 0014. By this rationale, claim 9 is rejected.

Regarding claims 10-11, 15-19, 30-31, 43, 47 the combination Dent-Tzamaloukas teaches:

10. The device of claim 9, wherein the various network layers include network layers in a protocol stack model selected from the group of: an OSI protocol stack model; an SS7 protocol stack model; and a TCP/IP protocol stack model (see Tzamaloukas; fig. 4; par. 0087).

11. The device of claim 9, wherein the various network layers include network layers selected from the group of:

a TCP port-level connection; a session level connection; a presentation level connection; an application level connection; a transaction capabilities application part level (TCAP) level connection; an integrated services digital network user part (ISUP) level connection; a mobile application part (MAP) level connection; and a signaling connection control point (SCCP) level connection (see Tzamaloukas; par.0087).

15. The computing device of claim 14, further including program instructions which execute to convert the network device to perform a different role (see Tzamaloukas; par. 0033, 0113).

16. The computing device of claim 15, further including program instructions which execute to convert a network database to serve as a network hub (see Tzamaloukas; par. 0033, 0113).

17. The computing device of claim 15, further including program instructions which execute to convert a network switch to a network hub(see Tzamaloukas; par. 0033, 0113).

18. The computing device of claim 12, further including program instructions which execute to track media access control (MAC) layer addressing and, based on applying the Kalman filter, execute to reduce false positives and false negatives (see Tzamaloukas, par. 0056, and 0076-0077; fig. 4).

19. The computing device of claim 12, further including program instructions which execute to track internet protocol (IP) flow and routing and, based on applying the Kalman filter, execute to reduce false positives and false negatives (see Tzamaloukas, par. 0056, and 0076-0077; fig. 4).

30. The method of claim 23, wherein the method includes: receiving information communicated between various network layers in a given protocol stack model; and learning network events based on applying the Kalman filter to the received information see Tzamaloukas, par. 0056, and 0076-0077; fig. 4).

31. The method of claim 23, wherein the method includes reducing false positives and false negatives based on applying the Kalman filter to received network information see Tzamaloukas, par. 0056, and 0076-0077; fig. 4).

43. The medium of claim 39, wherein the method further includes converting the network device from a first role to a second role based on applying the Kalman filter to received network information (see Tzamaloukas; par. 0033, 0113).

47. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to convert the network device to a different role (see Tzamaloukas; par. 0033, 0113).

Conclusion

6. ***This action is made Non-Final***. Any inquiry concerning this communication or earlier communications from examiner should be directed to Jude Jean-Gilles whose telephone number is (571) 272-3914. The examiner can normally be reached on Monday-Thursday and every other Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn, can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-3301.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-0800.

/Jude J Jean-Gilles/

Primary Examiner, Art Unit 2143

JJG

May 11, 2008